User's Manual
Wireless G Plus MIMO Router
F5D9230-4

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

The specification is subject to change without notice.

Table of Contents

Chapter 1　　Introduction

Congratulations on your purchase of this outstanding Wireless Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

Functions and Features

Router Basic functions

- **Auto-sensing Ethernet Switch**

  Equipped with a 4-port auto-sensing Ethernet switch.

- **WAN type supported**

  The router supports some WAN types, Static, Dynamic, PPPoE , PPTP ,L2TP, Dynamic IP with Road Runner.

- **Firewall**

  All unwanted packets from outside intruders are blocked to protect your Intranet.

- **DHCP server supported**

  All of the networked computers can retrieve TCP/IP settings automatically from this product.

- **Web-based configuring**

  Configurable through any networked computer's web browser using Netscape or Internet Explorer.

- **Virtual Server supported**

  Enable you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.

- **User-Definable Application Sensing Tunnel**

  User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then this product can sense the application type and open multi-port tunnel for it.

- **DMZ Host supported**

  Lets a networked computer be fully exposed to the Internet; this function is used when special application sensing tunnel feature is insufficient to allow an application to function correctly.

- **Statistics of WAN Supported**

  Enables you to monitor inbound and outbound packets

Wireless functions

- **High speed for wireless LAN connection**

  Up to 54Mbps data rate by incorporating Orthogonal Frequency Division Multiplexing (OFDM).

- **Roaming**

  Provides seamless roaming within the IEEE 802.11b (11M) and IEEE 802.11g (54M) WLAN infrastructure.

- **IEEE 802.11b compatible (11M)**

  Allowing inter-operation among multiple vendors.

- **IEEE 802.11g compatible (54M)**

  Allowing inter-operation among multiple vendors.

- **Auto fallback**

  54M, 48M, 36M, 24M, 18M, 12M, 6M data rate with auto fallback in 802.11g mode.

  11M, 5.5M, 2M, 1M data rate with auto fallback in 802.11b mode.

Security functions

- **Packet filter supported**

  Packet Filter allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

- **Domain Filter Supported**

  Let you prevent users under this device from accessing specific URLs.

- **URL Blocking Supported**

  URL Blocking can block hundreds of websites connection by simply a **keyword**.

- **VPN Pass-through**

  The router also supports VPN pass-through.

- **802.1X supported**

  When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.

- **Support WPA-PSK and WPA version 1 and 2**

  When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service

- **SPI Mode Supported**

  When SPI Mode is enabled, the router will check every incoming packet to detect if this packet is valid.

- **DoS Attack Detection Supported**

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

Advanced functions

- **System time Supported**

  Allow you to synchronize system time with network time server.

- **E-mail Alert Supported**

  The router can send its info by mail.

- **Dynamic dns Supported**

  At present,the router has 3 ddns.dyndns,TZO.com and dhs.org.

- **SNMP Supported**

  The router supports basic SNMP function.

- **Routing Table Supported**

  Now, the router supports static routing.

- **Schedule Rule supported**

  Customers can control some functions, like virtual server and packet filters when to access or when to block.

Other functions

- **UPNP (Universal Plug and Play)Supported**

  The router also supports this function. The applications: X-box, Msn Messenger.

Packing List

- Wireless broadband router unit
- Installation CD-ROM
- Power adapter
- CAT-5 UTP Fast Ethernet cable

Chapter 2   Hardware Installation

2.1 Panel Layout

2.1.1. Front Panel

Figure 2-1 Front Panel

LED: Ports:

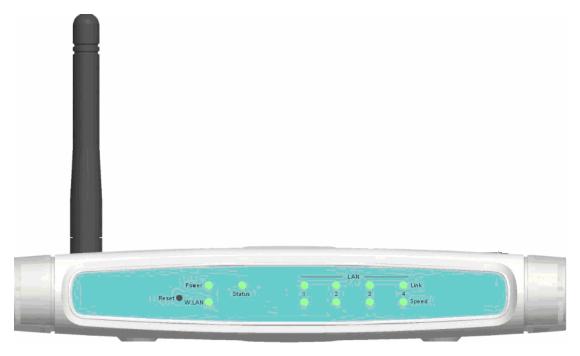| Port	Description
PWR	Power inlet
WAN	the port where you will connect your cable (or DSL) modem or Ethernet router.
Port 1-4	the ports where you will connect networked computers and other devices.

2.1.2. Rear Panel

Figure 2-2 Rear Panel

LED:

LED	Function	Color	Status	Description
Power	Power indication	Green	On	Power is being applied to this product.
Status	System status	Green	Blinking	Status is flashed once per second to indicate system is alive.
WAN	WAN port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
WLAN	Wireless activity	Green	Blinking	Sending or receiving data via wireless
Link. 1~4	Link status	Green	On	An active station is connected to the corresponding LAN port.
Speed 10/100	Data Rate	Green	Blinking	The corresponding LAN port is sending or receiving data.
			On	Data is transmitting in 100Mbps on the corresponding LAN port.
Reset				To reset system settings to factory defaults

2.2 Procedure for Hardware Installation

2. **Decide where to place your Wireless Broadband Router**

You can place your Wireless Broadband Router on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

2. **Setup LAN connection**

   a. Wired LAN connection: connects an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.

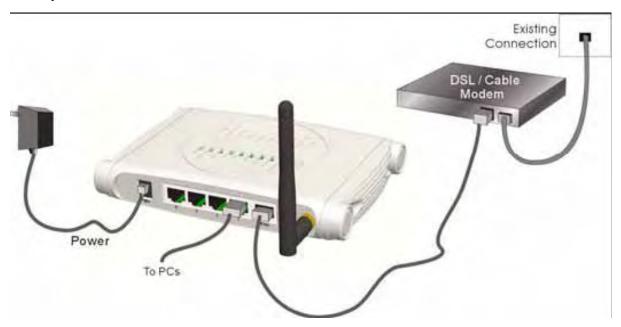   **b.** Wireless LAN connection: locate this product at a proper position to gain the best transmit performance.

Figure 2-3 Setup of LAN and WAN connections for this product.

3. **Setup WAN connection**

   Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone. Figure 2-3 illustrates the WAN connection.

4. **Power on**

   Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the indicators M1 will be lighted ON for about 10 seconds, and then M1 will be flashed 3 times to indicate that the self-test operation has finished. Finally, the M1 will be continuously flashed once per second to indicate that this product is in normal operation.

Chapter 3 Network Settings and Software Installation

To use this product correctly, you have to properly configure the network settings of your computers and install the attached setup program into your MS Windows platform (Windows 95/98/NT/2000).

3.1 Make Correct Network Settings of Your Computer

The default IP address of this product is 192.168.123.254, and the default subnet mask is 255.255.255.0. These addresses can be changed on your need, but the default values are used in this manual. If the TCP/IP environment of your computer has not yet been configured, you can refer to **Appendix A** to configure it. For example,

1. configure IP as 192.168.123.1, subnet mask as 255.255.255.0 and gateway as 192.168.123.254, or more easier,

2. configure your computers to load TCP/IP setting automatically, that is, via DHCP server of this product.

After installing the TCP/IP communication protocol, you can use the **ping** command to check if your computer has successfully connected to this product. The following example shows the ping procedure for Windows 95 platforms. First, execute the **ping** command

> **ping 192.168.123.254**

If the following messages appear:

> **Pinging 192.168.123.254 with 32 bytes of data:**

> **Reply from 192.168.123.254: bytes=32 time=2ms TTL=64**

a communication link between your computer and this product has been successfully established. Otherwise, if you get the following messages,

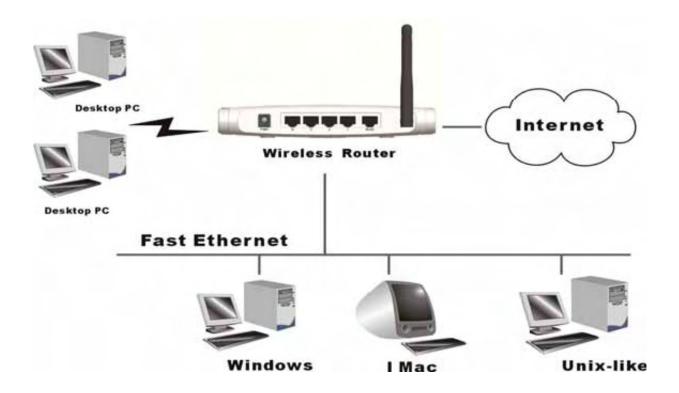> **Pinging 192.168.123.254 with 32 bytes of data:**

> **Request timed out.**

There must be something wrong in your installation procedure. You have to check the following items in sequence:

1. Is the Ethernet cable correctly connected between this product and your computer?

    Tip: The LAN LED of this product and the link LED of network card on your computer must be lighted.

2. Is the TCP/IP environment of your computers properly configured?

    Tip: If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

Chapter 4 Configuring Wireless Broadband Router

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Netscape Communicator or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.
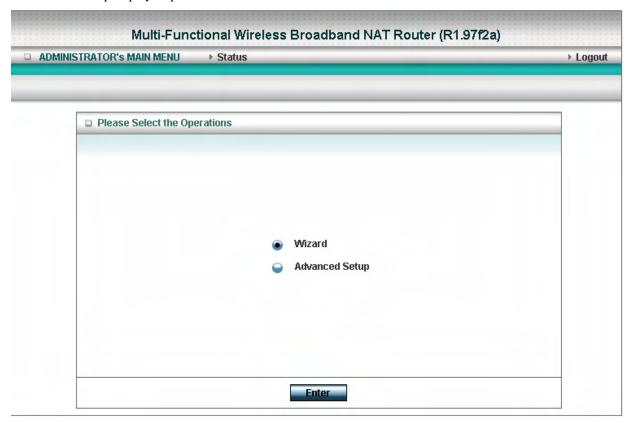
4.1 Login to Configure from Wizard

Activate your browser, and **disable the proxy** or **add the IP address of this product into the exceptions**. Then, type this product's IP address in the Location (for Netscape) or Address (for IE) field and press ENTER. For example: **http://192.168.123.254**.
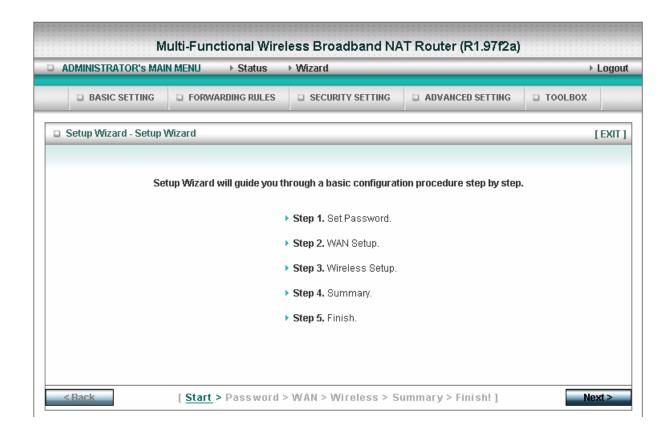
After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

To log in as an administrator, enter the system password (the factory setting is ''**admin**'') in the **System Password** field and click on the **Log in** button. If the password is correct, the web appearance will be changed into administrator configure mode. As listed in its main menu, there are several options for system administration.
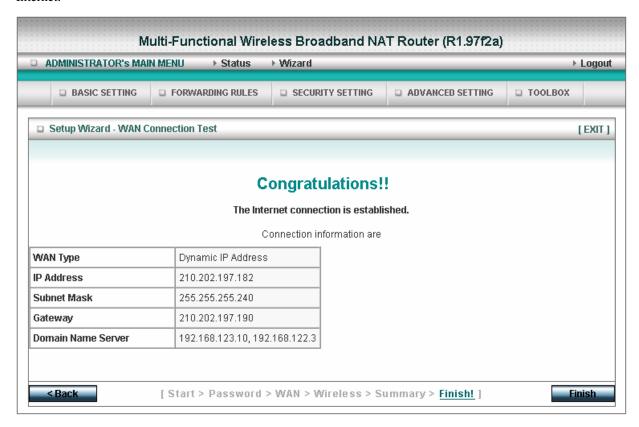
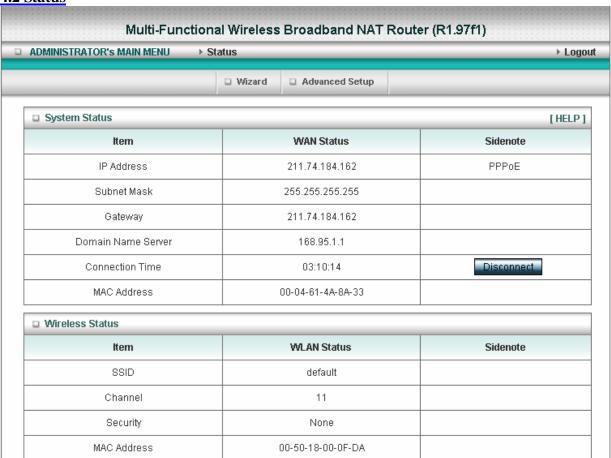The user can setup step by step to finish the connection with Wizard.

Setup Wizard will guide you through a basic configuration procedure step by step.Press **''Next >''**

If the user finishes those steps and the router shows as below. It means that customers can enjoy Internet.

4.2 Status

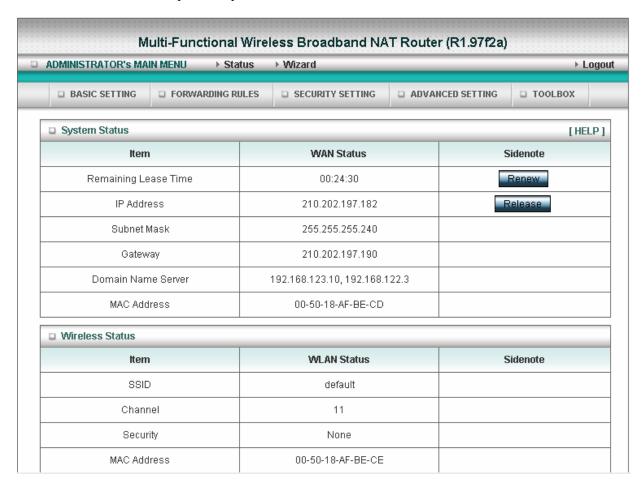This option provides the function for observing this product's working status:

A. WAN Port Status.

   If the WAN port is assigned a dynamic IP, there may appear a "**Renew**" or "**Release**" button on the Sidenote column. You can click this button to renew or release IP manually.
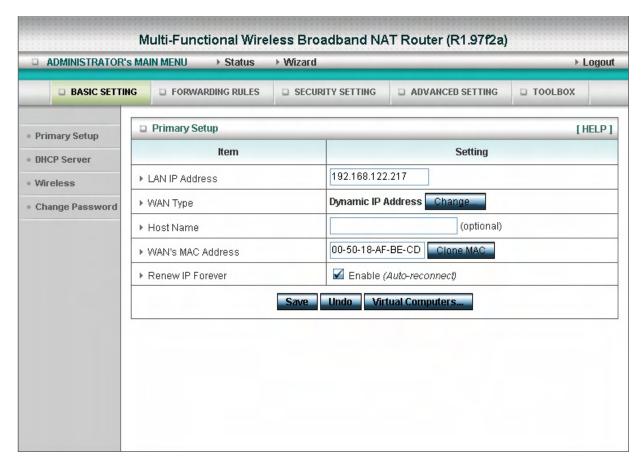
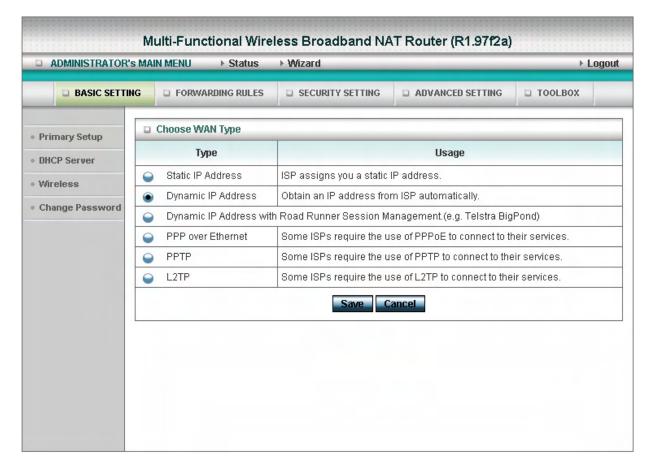B. Statistics of WAN: enables you to monitor inbound and outbound packets

4.4 Basic Setting

Please Select "Advanced Setup" to Setup

4.4.1 Primary Setup – WAN Type, Virtual Computers

Press **"Change"**

This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

1. **LAN IP Address**: the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.

2. **WAN Type**: WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:

   A.   Static IP Address: ISP assigns you a static IP address.

   B.   Dynamic IP Address: Obtain an IP address from ISP automatically.

   C.   Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)

   D.   PPP over Ethernet: Some ISPs require the use of   PPPoE to connect to their services.

   E.   PPTP: Some ISPs require the use of   PPTP to connect to their services.

   F.   L2TP: Some ISPs require the use of   L2TP to connect to their services

4.4.1.1 Static IP Address

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

4.4.1.2 Dynamic IP Address

1. Host Name: optional. Required by some ISPs, for example, @Home.

2. Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

4.4.1.3 Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)

1. LAN IP Address is the IP address of this product. It must be the default gateway of your computers.

2. WAN Type is Dynamic IP Address. If the WAN type is not correct, change it!

3. Host Name: optional. Required by some ISPs, e.g. @Home.

4. Renew IP Forever: this feature enable this product renew IP address automatically when the lease time is being expired even the system is in idle state.

4.4.1.4 PPP over Ethernet

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.
4. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The most common MTU value is 1492.
5. Connection Control:There are 3 modes to select:

   Connect-on-demand:The device will link up with ISP when the clients send outgoing packets.

   Auto-Reconnect(Always-on):The device will link upw with ISP until the connection is established.

   Manually:The device will not make the link until someone clicks the connect-button in the Staus-page.
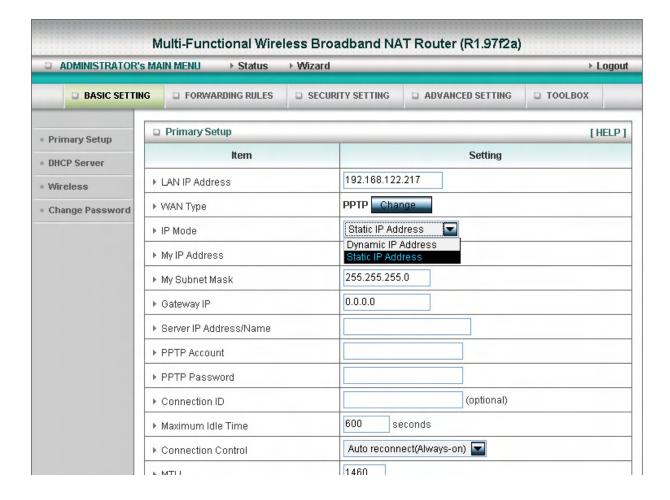
4.4.1.5 PPTP

First,Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

1.   My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned

to you.

2.   Server IP Address: the IP address of the PPTP server.

3.   PPTP Account and Password: the account and password your ISP assigned to you. If you don't

want to change the password, keep it empty.

3.   Connection ID: optional. Input the connection ID if your ISP requires it.

4.   Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or

enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will

connect to ISP automatically, after system is restarted or connection is dropped.

5.   Connection Control:There are 3 modes to select:

Connect-on-demand:The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on):The device will link upw with ISP until the connection is established.

Manually:The device will not make the link until someone clicks the connect-button in the

Staus-page.

4.4.1.6 L2TP

First,Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

For example:Use Static

1.   My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned

      to you.

2.   Server IP Address: the IP address of the PPTP server.

3.   PPTP Account and Password: the account and password your ISP assigned to you. If you don't

      want to change the password, keep it empty.

3.   Connection ID: optional. Input the connection ID if your ISP requires it.

4.   Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or

      enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will
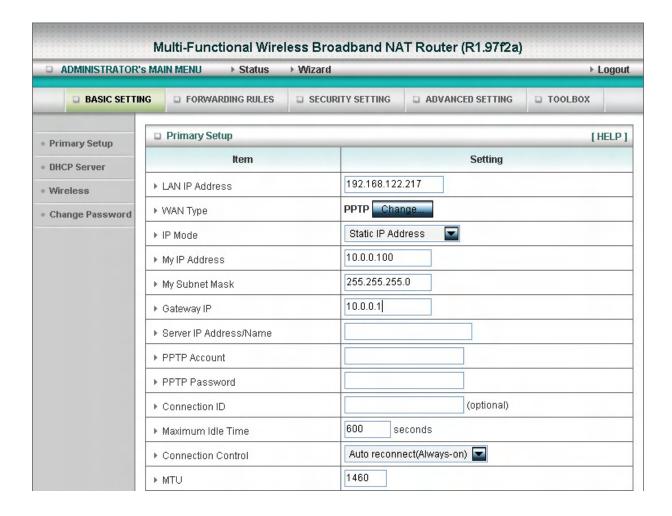
connect to ISP automatically, after system is restarted or connection is dropped.
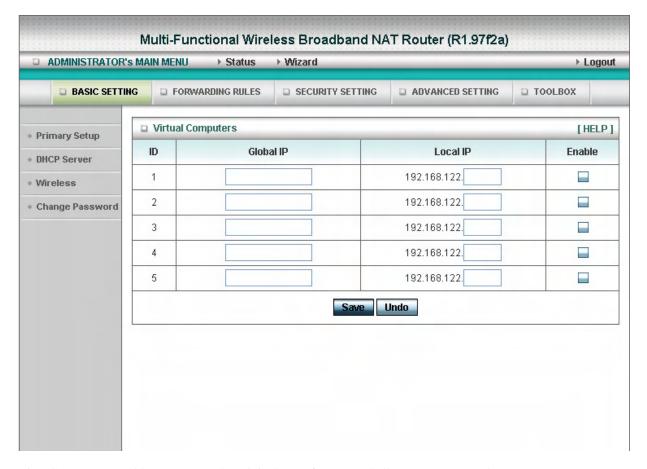
6.   Connection Control:There are 3 modes to select:

Connect-on-demand:The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on):The device will link upw with ISP until the connection is established.

Manually:The device will not make the link until someone clicks the connect-button in the
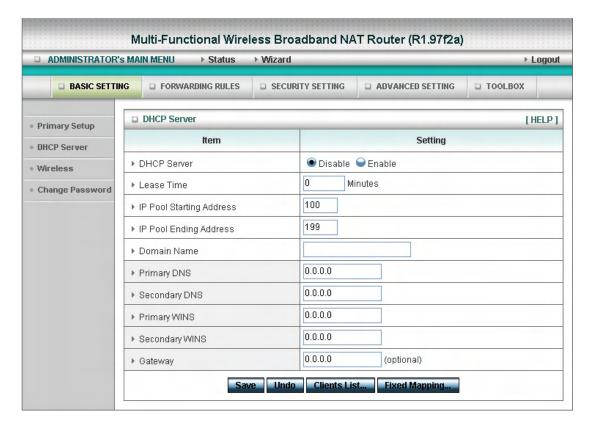   Staus-page.

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

| □ BASIC SETTING | □ FORWARDING RULES | □ SECURITY SETTING | □ ADVANCED SETTING | □ TOOLBOX |

- Primary Setup
- DHCP Server
- Wireless
- Change Password

□ Primary Setup   [HELP]

Item	Setting
▸ LAN IP Address	192.168.122.217
▸ WAN Type	**PPTP** Change...
▸ IP Mode	Static IP Address ▾
▸ My IP Address	10.0.0.100
▸ My Subnet Mask	255.255.255.0
▸ Gateway IP	10.0.0.1
▸ Server IP Address/Name	
▸ PPTP Account	
▸ PPTP Password	
▸ Connection ID	(optional)
▸ Maximum Idle Time	600 seconds
▸ Connection Control	Auto reconnect(Always-on) ▾
▸ MTU	1460

4.4.1.7 Virtual Computers(Only for Static and dynamic IP address Wan type)

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- Global IP: Enter the global IP address assigned by your ISP.
- Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.
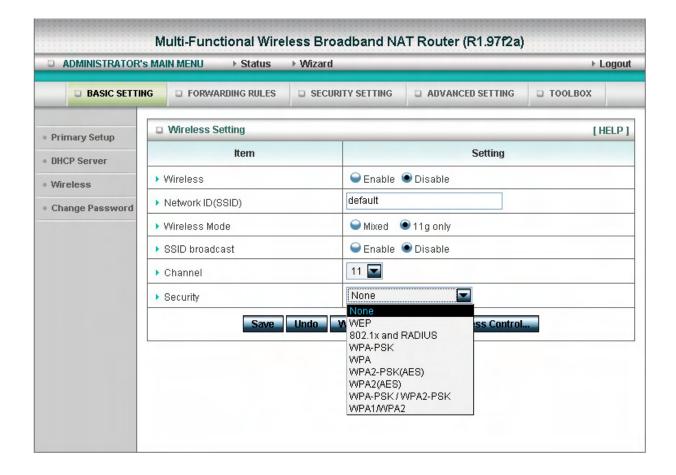- Enable: Check this item to enable the Virtual Computer feature.

4.4.2 DHCP Server

Press **"More>>"**

The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations. It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the function of DHCP server. If you enable this product's DHCP server and configure your computers as "automatic IP allocation" mode, then when your computer is powered on, it will automatically load the proper TCP/IP settings from this product. The settings of DHCP server include the following items:

1. **DHCP Server**: Choose "Disable" or "Enable."

2. **IP pool starting Address/ IP pool starting Address**: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

3. **Domain Name**: Optional, this information will be passed to the client.

4. **Primary DNS/Secondary DNS**: This feature allows you to assign DNS Servers

5. **Primary WINS/Secondary WINS**: This feature allows you to assign WINS Servers

6. **Gateway**: The Gateway Address would be the IP address of an alternate Gateway.
    This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

4.4.3 Wireless Setting, 802.1X setting and WDS

Wireless settings allow you to set the wireless configuration items.

Wireless : The user can enable or disalbe wireless function.

Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is "**default**")

SSID Broadcast: The router will Broadcast beacons that have some information, including ssid so that The wireless clients can know how many ap devices by scanning function in the network. Therefore, This function is disabled, the wireless clients can not find the device from beacons.

Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory setting is as follow: **channel 6** for North America; **channel 7** for European (ETSI); **channel 7** for Japan.

Security: Select the data privacy algorithm you want. Enabling the security can protect your data while

it is transferred from one station to another.

There are several security types to use:

WEP :

When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.
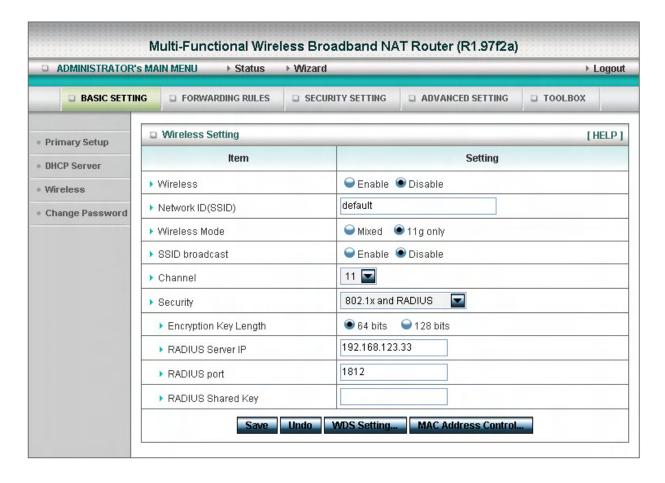
802.1X

Check Box was used to switch the function of the 802.1X. When the 802.1X function is enabled, the Wireless user must **authenticate** to this router first to use the Network service.
RADIUS Server

IP address or the 802.1X server's domain-name.
RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.
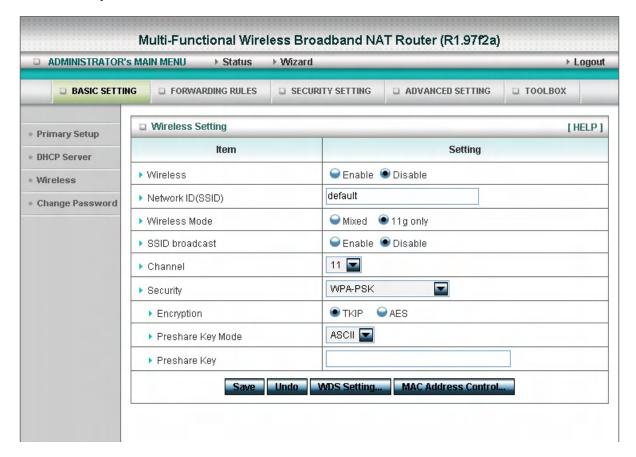
WPA-PSK

1. Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server
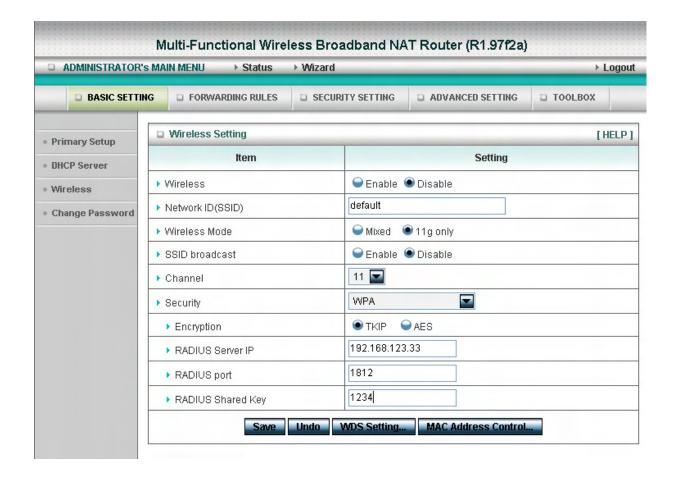
IP address or the 802.1X server's domain-name.
Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.
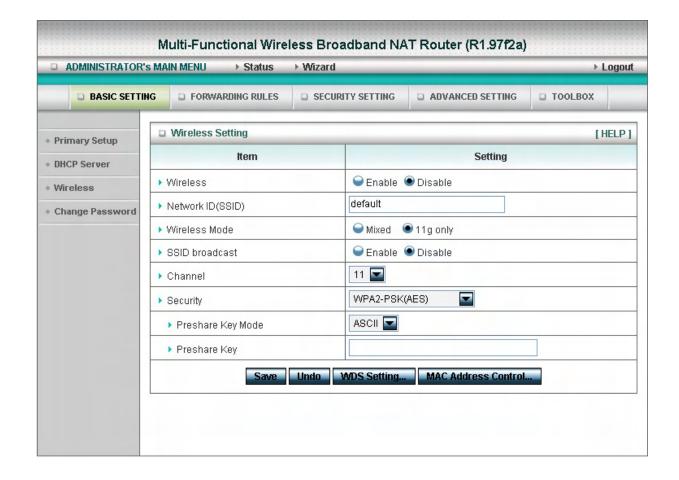
WPA2-PSK(AES)

1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

WPA2(AES)

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server
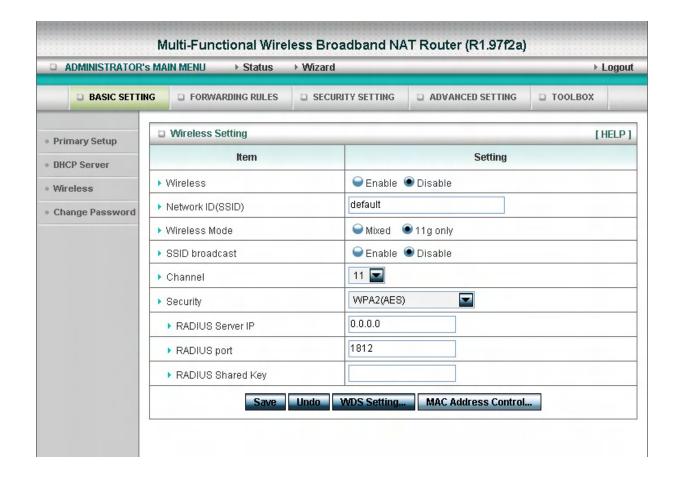
IP address or the 802.1X server's domain-name.

Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.
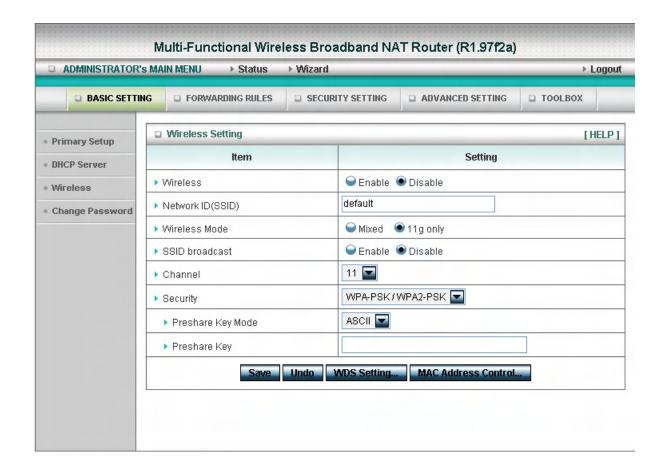
WPA-PSK /WPA2-PSK

The router will detect automatically   which Security type the client

uses to encrypt.

1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

WPA/WPA2

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server

The router will detect automatically   which Security type(Wpa-psk version 1 or 2) the client

uses to encrypt.
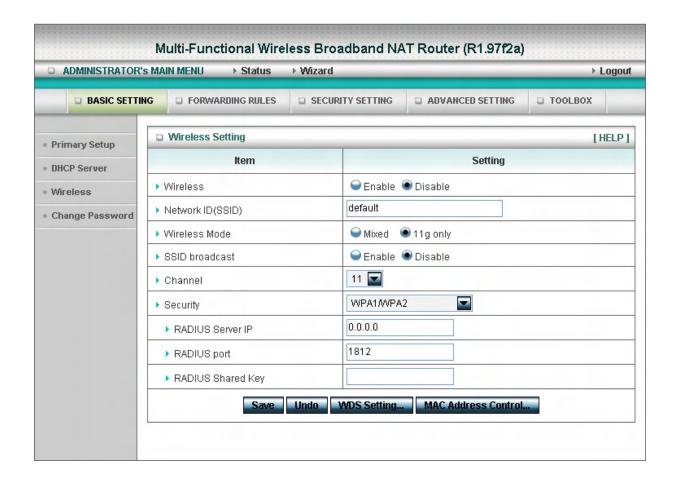
IP address or the 802.1X server's domain-name.

Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

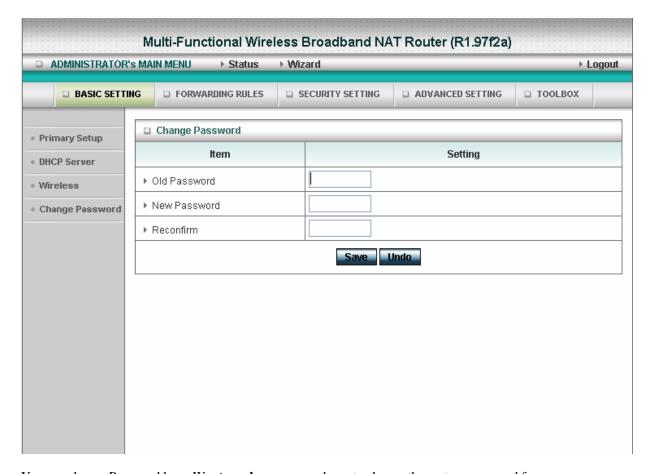Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WDS(Wireless Distribution System)

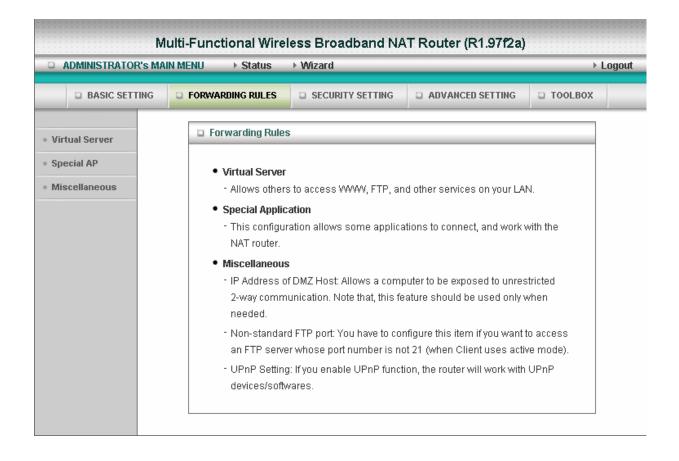WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.
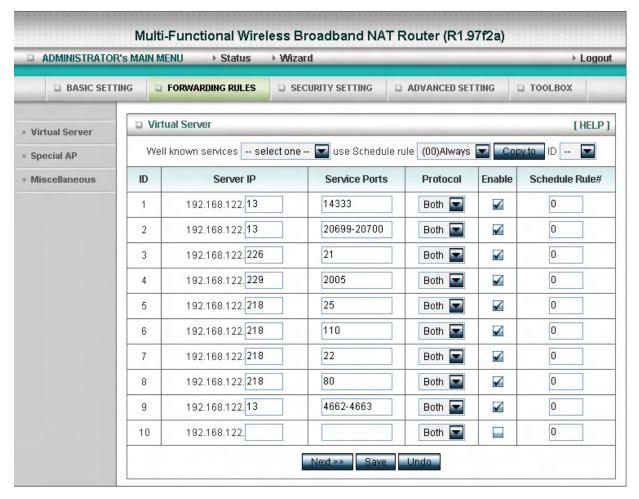
4.4.4 Change Password

You can change Password here. We **strongly** recommend you to change the system password for security reason.

4.5 Forwarding Rules

4.5.1 Virtual Server

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**.   **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

4.5.2 Special AP

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

1. **Trigger**: the outbound port number issued by the application..

2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings Select your application and click **Copy to** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

4.5.3 Miscellaneous Items

IP Address of DMZ Host

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.
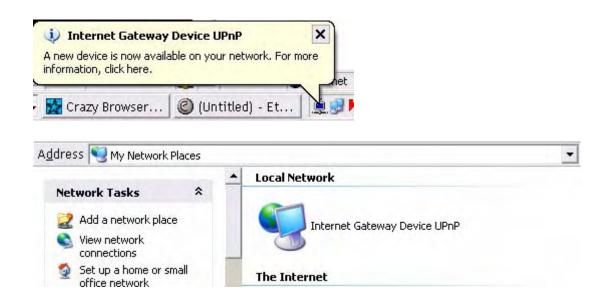
Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

UpnP Setting

The device also supports this function.If the OS supports this function enable it,like Windows Xp.When the user get ip from Device and will see icon as below:

4.6 Security Settings

4.6.1 Packet Filter

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. **Packet Filter** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

Each rule can be enabled or disabled individually.

Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the **Inbound Packet Filter** field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

Example 1:

(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110), and browse the Internet (port 80)

(1.2.3.10-1.2.3.20) They can do everything (block nothing)

Others are all blocked.
Example 2:

(1.2.3.100-1.2.3.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)
Others are all allowed.

After **Inbound Packet Filter** setting is configured, click the **save** button.

Outbound Filter:

To enable **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

Example 1:

☐ BASIC SETTING	☐ FORWARDING RULES	☐ **SECURITY SETTING**	☐ ADVANCED SETTING	☐ TOOLBOX

- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

☐ Inbound Packet Filter [HELP]

Item	Setting
▶ Inbound Filter	☑ Enable

◉ Allow all to pass except those match the following rules.
◯ Deny all to pass except those match the following rules.

Schedule rule (00)Always ▼ [Copy to] ID -- ▼

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	192.168.123.149 :	: 25-100	☑	0
2	192.168.123.20 :	:	☑	0
3	:	:	☐	0
4	:	:	☐	0
5	:	:	☐	0
6	:	:	☐	0
7	:	:	☐	0
8	:	:	☐	0

[Save] [Undo] [Outbound Filter...] [MAC Level...]

(192.168.123.100-192.168.123.149) They are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.123.10-192.168.123.20) They can do everything (block nothing)
Others are all blocked.

Example 2:

| | BASIC SETTING | | FORWARDING RULES | | SECURITY SETTING | | ADVANCED SETTING | | TOOLBOX |

- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

Inbound Packet Filter   [HELP]

Item	Setting
▶ Inbound Filter	☑ Enable
	⦿ Allow all to pass except those match the following rules. ◯ Deny all to pass except those match the following rules.
	Schedule rule (00)Always ▼ Copy to ID -- ▼

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	192.168.123.100 :	: 21	☑	0
2	192.168.123.119 :	: 119	☑	0
3	:	:	☐	0
4	:	:	☐	0
5	:	:	☐	0
6	:	:	☐	0
7	:	:	☐	0
8	:	:	☐	0

Save   Undo   Outbound Filter...   MAC Level...

(192.168.123.100-192.168.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

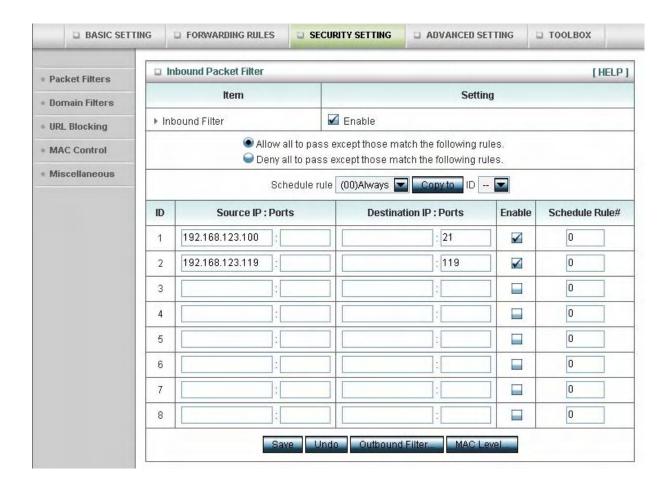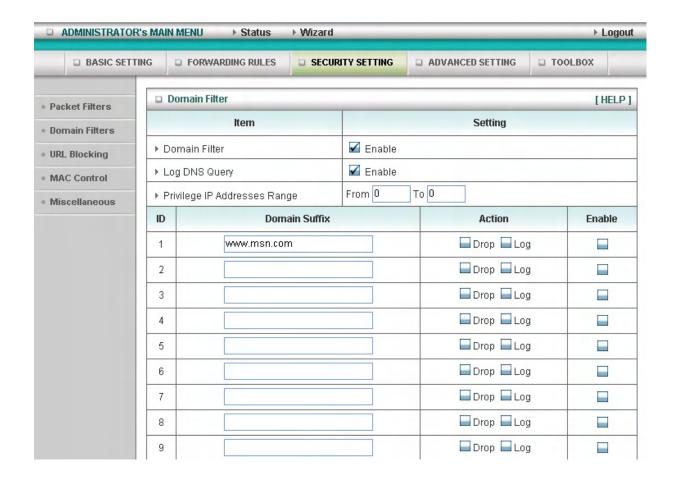After **Outbound Packet Filter** setting is configured, click the **save** button.

4.6.2 Domain Filter

Domain Filter

Let you prevent users under this device from accessing specific URLs.

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Addresses Range

Setting a group of hosts and privilege these hosts to access network without restriction.

Domain Suffix

A suffix of URL to be restricted. For example, ".com", "xxx.com".
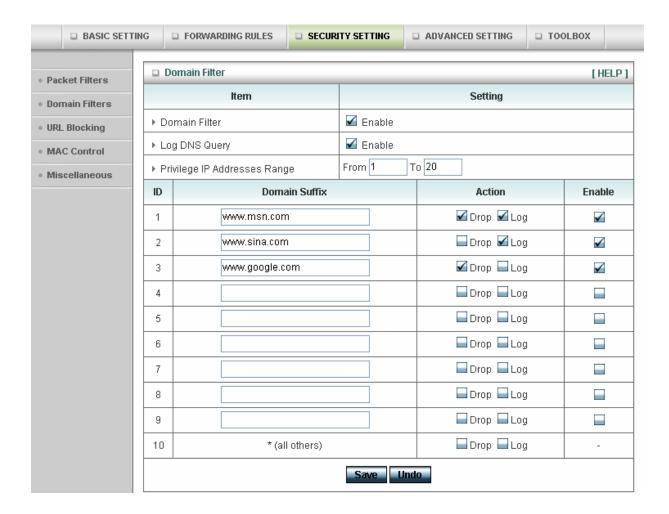
Action

When someone is accessing the URL met the domain-suffix, what kind of action you want.

Check drop to block the access. Check log to log these access.
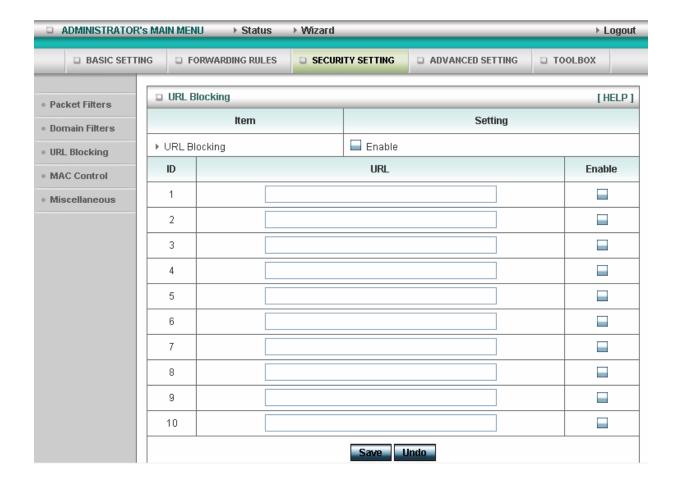
Enable

Check to enable each rule.

Example:

In this example:

1. URL include "www.msn.com" will be blocked, and the action will be record in log-file.

2. URL include "www.sina.com" will not be blocked, but the action will be record in log-file.

3. URL include "www.google.com" will be blocked, but the action will not be record in log-file.

4. IP address X.X.X.1~ X.X.X.20 can access network without restriction.

4.6.3 URL Blocking

URL Blocking will block LAN computers to connect to pre-defined Websites.

The major difference between "Domain filter" and "URL Blocking" is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.
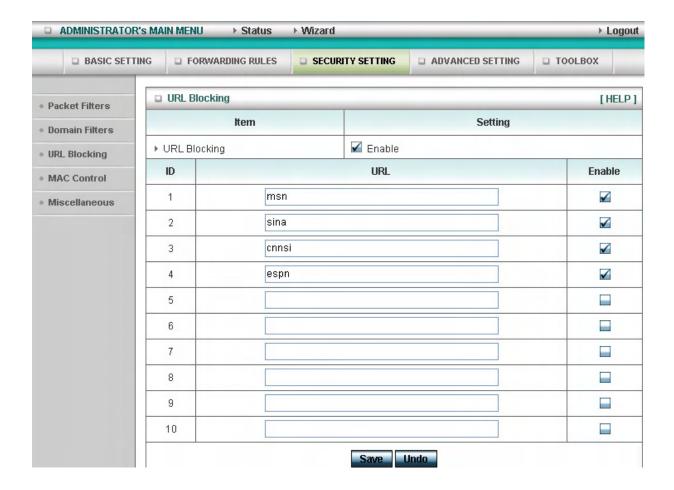
URL Blocking Enable

Checked if you want to enable URL Blocking.

URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".
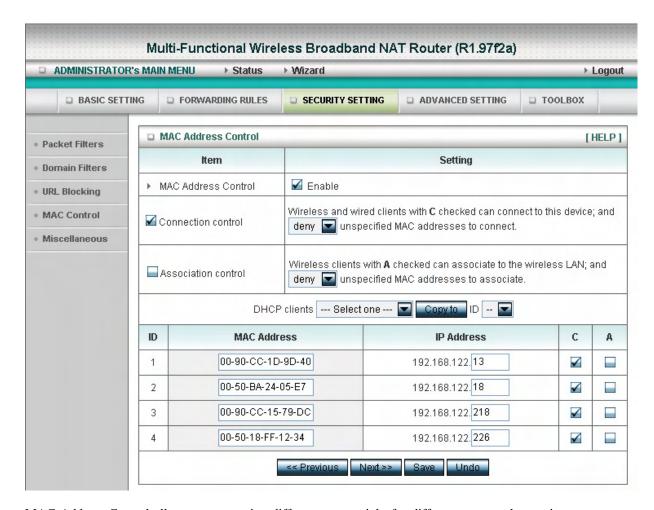
Enable

Checked to enable each rule.

In this example:

1. URL include "msn" will be blocked, and the action will be record in log-file.

2. URL include "sina" will be blocked, but the action will be record in log-file

3. URL include "cnnsi" will not be blocked, but the action will be record in log-file.

4. URL include "espn" will be blocked, but the action will be record in log-file

4.6.4 MAC Address Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

MAC Address Control	Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.
Connection control	Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.
Association control	Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data

via this device. Choose "allow" or "deny" to
allow or deny the clients, whose MAC
addresses are not in the "Control table", to
associate to the wireless LAN.

Control table

ID	MAC Address	IP Address	C	A
9		192.168.122.		
10		192.168.122.		
11		192.168.122.		
12		192.168.122.		

"Control table" is the table at the bottom of the "MAC Address Control"
page. Each row of this table indicates the MAC address and the expected
IP address mapping of a client. There are four columns in this table:

MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
C	When "**Connection control**" is checked, check "**C**" will allow the corresponding client to connect to this device.
A	When "**Association control**" is checked, check "**A**" will allow the corresponding client to associate to the wireless LAN.

In this page, we provide the following Combobox and button to help you to input the MAC address.

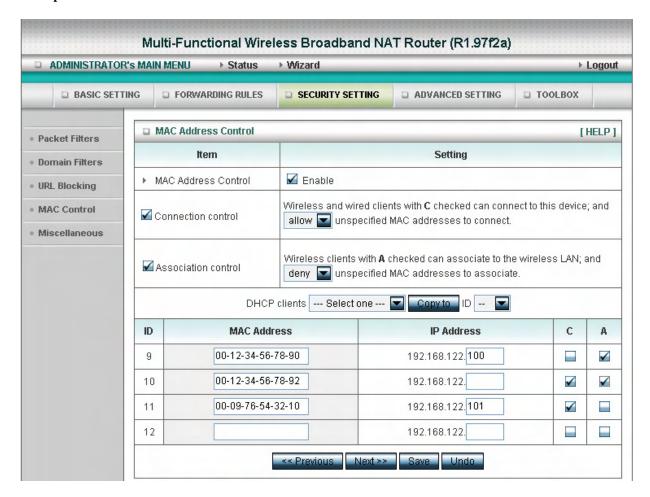DHCP clients | -- select one -- ▼ | Copy to | ID | -- ▼ |

You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to"
button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

Previous page and Next Page   To make this setup page simple and clear, we have divided the
"Control table" into several pages. You can use these buttons to
navigate to different pages.

Example:

In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.
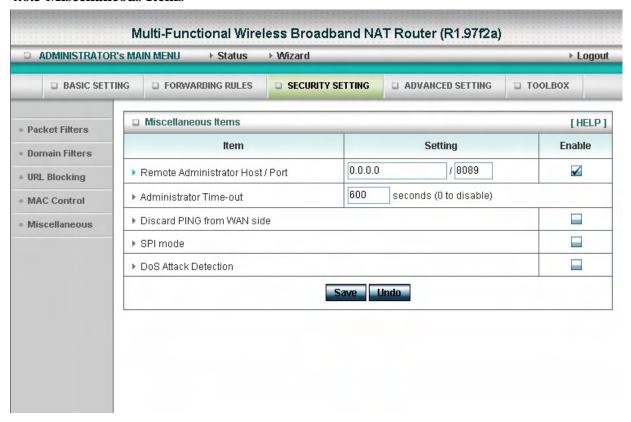
1. The "MAC Address Control" function is enabled.

2. "Connection control" is enabled, and all of the wired and wireless clients not listed in the "Control table" are "allowed" to connect to this device.

3. "Association control" is enabled, and all of the wireless clients not listed in the "Control table" are "denied" to associate to the wireless LAN.

4. Clients 1 and 3 have fixed IP addresses either from the DHCP server of this device or manually assigned:

   ID 1 - "00-12-34-56-78-90" --> 192.168.122.100

   ID 3 - "00-98-76-54-32-10" --> 192.168.122.101

   Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.

   If, for example, client 3 tries to use an IP address different from the address listed in the Control table (192.168.122.101), it will be denied to connect to this device.

5.Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.

6.Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

4.6.5 Miscellaneous Items

Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.

Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

SPI Mode

When this feature is enabled, the router will record the packet information pass through the router like

IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

DoS Attack Detection

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

4.7 Advanced Settings